1 Question 1

1.1 Part a

$$P = (C \boxplus \bar{K_1}) \oplus K_0$$

where $\bar{K_1}$ is the complement of K_1.

1.2 Part b

Let our plaintext messages be P_a, P_b and their corresponding ciphertexts be C_a, C_b. We know that

$$C_a = (P_a \oplus K_0) \boxplus K_1$$
$$C_b = (P_b \oplus K_0) \boxplus K_1$$

We can define K_0 in terms of C_a, P_a, and K_1 by rearranging the variables.

$$(P_a \oplus K_0) \boxplus K_1 = C_a$$

$$P_a \oplus K_0 = C_a \boxplus \bar{K_1}$$
$$K_0 = (C_a \boxplus \bar{K_1}) \oplus P_a$$

Likewise,

$$K_0 = (C_b \boxplus \bar{K_1}) \oplus P_b$$

Which means

$$(C_a \boxplus \bar{K_1}) \oplus P_a = (C_b \boxplus \bar{K_1}) \oplus P_b$$
$$(C_a \boxplus \bar{K_1}) \oplus P_a \oplus P_b = C_b \boxplus \bar{K_1}$$
$$\big((C_a \boxplus \bar{K_1}) \oplus P_a \oplus P_b\big) \boxplus C_b = \bar{K_1}$$

We can then use $\bar{K_1}$ to find K_0 via

$$K_0 = (C_a \boxplus \bar{K_1}) \oplus P_a$$

2 Question 2

I will solve this problem for the general case. Let me denote the encryption of message m as $E(m)$, since the key is not relevent here. The defined encryption scheme being linear means

$$E(m_a) \oplus E(m_b) = E(m_a \oplus m_b)$$

This also implies that a message made of all zeroes will be encrypted to a message of all zeroes.

Now, let each input m_i and corresponding output $E(m_i)$ be l bits long. Choose l ciphertexts $E(m_i)$ such that

$$E(m_1) = 1000\ldots$$

$$E(m_2) = 0100\ldots$$

$$E(m_3) = 0010\dots$$
$$\dots$$
$$E(m_{l-1}) = \dots 0010$$
$$E(m_l) = \dots 0001$$

I denote this set $\mathscr{E}$. If I know the corresponding plaintexts $\{m_1, m_2, \dots m_l\}$, I can decipher any message using the linear property of E. Let $E(m_k)$ be an intercepted message. $E(m_k$ can be described by XORing a unique subset of $\mathscr{E}$. Now becuase of the linear property of E, I can retreive m_k by XORing the m's that correspond to the aforementioned unique subset.

For example, let

$$E(m_k) = E(m_1) \oplus E(m_{17}) \oplus E(m_{42})$$

We can retrieve m_k via

$$m_k = m_1 \oplus m_{17} \oplus m_{42}$$